



Conews

FORUM 2014

СОБЫТИЯ И ТЕНДЕНЦИИ В СФЕРЕ ИБ

Денис Легезо

БЕСПРЕЦЕДЕНТНАЯ УЯЗВИМОСТЬ OPENSSL



Уязвимость оставалась незамеченной **два года**

Среди уязвимых Apache, nginx. Сервисы Yahoo Mail, Facebook

ЦЕЛЕВАЯ АТАКА DARK HOTEL



Конкретным
постояльцам предлагают
установить обновления
Adobe, Google

Сертификаты не
похищались, а
подделывались после
атаки на слабые 512
битные ключи

Интересный **кейлогер**

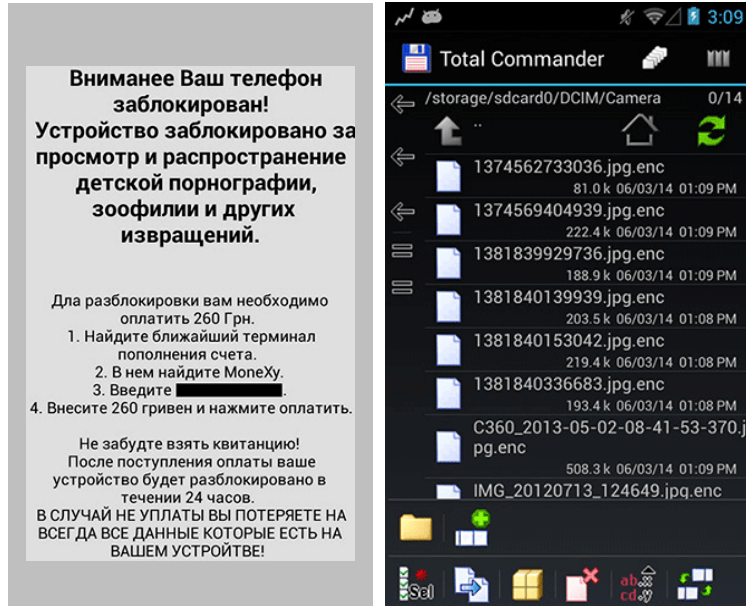
ОБЕЗОБРАЖЕННОЕ ЛИЦО

```
erride à...€@S,f...Z`€t,, Proxy Server ...€@fS@...Z1^^ Proxy Enabled @@@`f...@f#@`@@,, [-]
IE Proxy configuration :...Z%€...Z€@`Zf...,@,,%...€...Z€@%€€ Unknown ,,,€€S...@ Installed in sy
tem32? t,,1%@Zf,@I@I%...1,$Z`...< No @Z $`€,,Z,,€I system32 €fTtI,Z€f% \ Filename €@
@€$Z€€ CLSID>{E0D4FC4D-521C-11D0-B792-00A0C90312E1}\InprocServer32 €ft%€%...`fS`€,,ftI`@
S@`tt,,ffZS`@f€,€fTt@,S@+T@€fZ, %S, @@@ [-]Installation Information: ,,@€€€@€,@,@@,@@,@@
...@S@%,f%`@€@`@ Careto - GetSystemReport v1.0 ,,€@I@...Z€f%@...I...€,,I1`€%`€...fI... SystemP
port.txt €t@€@+t,€€@€S€<€ SetCngLog.txt I @Z€€S@€@Z@ %s (%s) New Configurati
n updated ONLY for current user @S€Z@+T@€@T@€T`ZS,,`€T,,, ,,%`€T,,,€...@Zf,@,€%`f
New Configuration updated for all users %,@f@,,tZ`fI@,Zf€,S<@...€I<€...Zt`f`€S@ New
MIN_ATTEMPS_URL_AUX=%d @`%@fS`tt,@t%Z€€, @€@t@€@%€ New URL_AUX_WAIT=%d days @f%€fttZ€
fZ<@%,f@,@t,, New URL_AUX=%s ,,€t<SSZ@+TZfS@ New URL_MAIN=%s €`@SZ€`tZ,@_@SŠ
Original MIN_ATTEMPS_URL_AUX=%d f€@€€fSf@€@€f€T@€@Z€,T$€@,€,€€t Original URL_AUX_WA
T=%d days @@...,,@€%...tZ@S...€@Z,@S@€€€ Original URL_AUX=%s %€t%@...<fS%Z<...SSt<,,
```

2014 год отметился наиболее
изощренной целевой атакой
Careto

Данные собирались с **2007**

РАЗВИТИЕ МОБИЛЬНЫХ УГРОЗ



Внимание Ваш телефон заблокирован!
Устройство заблокировано за просмотр и распространение детской порнографии, зоофилии и других извращений.

Для разблокировки вам необходимо оплатить 260 Грн.

1. Найдите ближайший терминал пополнения счета.
2. В нем найдите МолеХу.
3. Введите [REDACTED].
4. Внесите 260 гривен и нажмите оплатить.

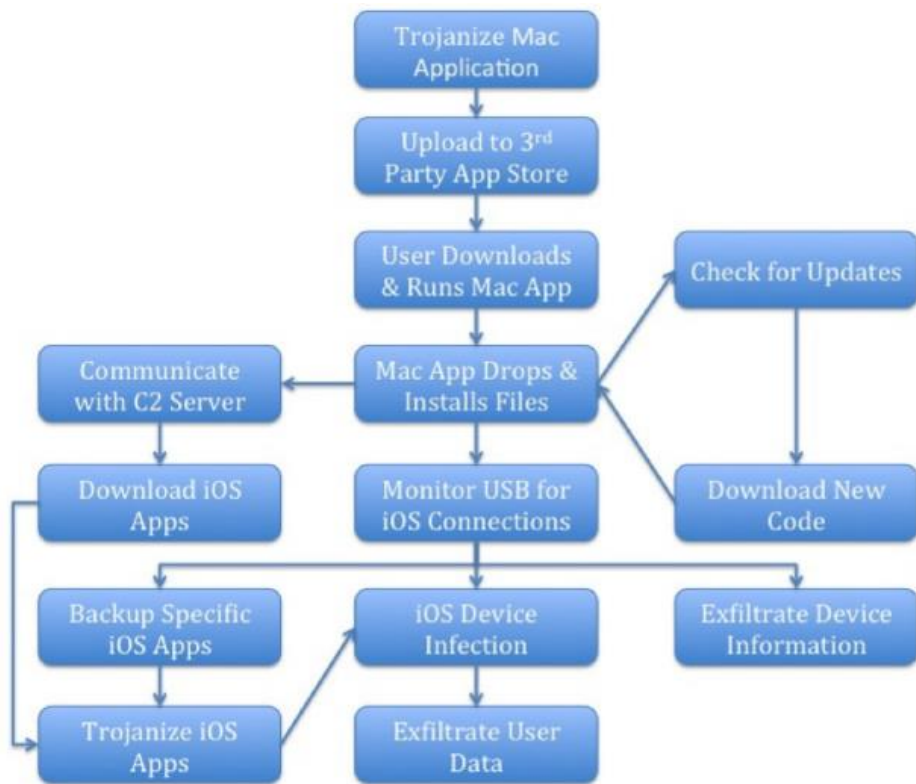
Не забудьте взять квитанцию!
После поступления оплаты ваше устройство будет разблокировано в течении 24 часов.
В СЛУЧАЕ НЕ УПЛАТЫ ВЫ ПОТЕРЯЕТЕ НА ВСЕГДА ВСЕ ДАННЫЕ КОТОРЫЕ ЕСТЬ НА ВАШЕМ УСТРОЙСТВЕ!

The screenshot shows the 'Total Commander' file manager interface on an Android device. The current directory is '/storage/sdcard0/DCIM/Camera'. The file list includes several '.jpg.enc' files with their sizes and timestamps, and a '.jpg' file named 'C360_2013-05-02-08-41-53-370.jpg'. The bottom dock contains icons for 'Sal', a folder, a document, a red 'X' icon, and a keyboard icon.

Появление первого шифровальщика-вымогателя под **Android**

WireLurker инфицирует подключенные к ПК **iOS-**устройства

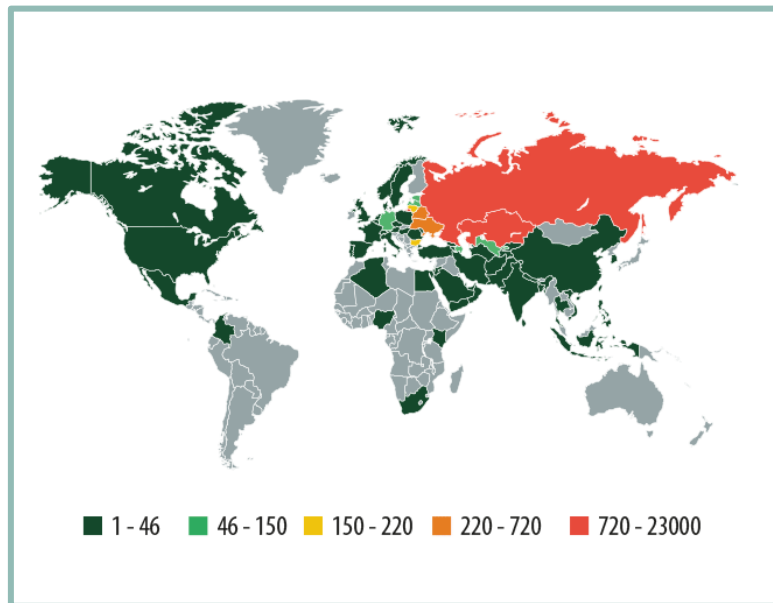
КАК РАБОТАЕТ WIRELURKER



Инфицируются мобильные устройства и **без jailbrake**

Приложение на ПК автоматически обновляется и **следит за подключениями** через USB-порт

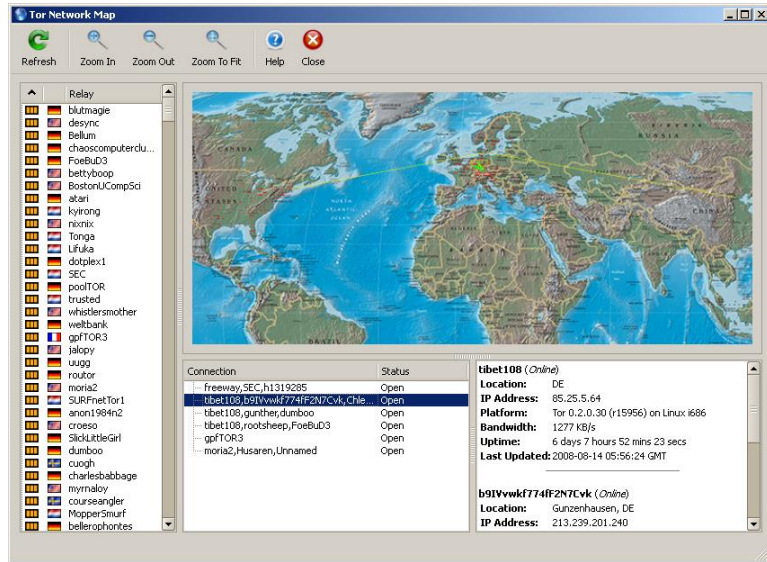
МОБИЛЬНЫЕ БАНКЕРЫ



Начало 2014 – около 1300
уникальных мобильных
банкеров

Конец Q1 – **уже 2500**

АНОНИМИЗАЦИЯ ЧЕРЕЗ TOR И BITCOIN



В 2014 появился первый троян для Android с **консолью управления в .onion**

“ГОДЗИЛЛА АТАКУЕТ!”



Дорожные знаки пострадали из-за **слабой аутентификации**: простых «общих строк» в протоколе SNMP